Showing Credentials Without Identification

Signatures Transferred Between Unconditionally Unlinkable Pseudonyms

David Chaum
Center for Mathematics and Computer Science (CWI)

Kruislaan 413, 1098 SJ Amsterdam, The Netherlands

EXTENDED SUMMARY

It is becoming increasingly easy and common for organizations to routinely exchange data on individuals. Because each individual provides most organizations essentially the same uniquely identifying information, such as social security number, or name, age and place of birth, the records held by one organization on an individual are readily matched or linked with those held by other organizations. Thus, organizations are capable of exchanging information about individuals whenever and to whatever extent they choose. Clearly some such transfers of information are quite useful and beneficial to society. The problems stem from the inability of anyone, particularly the individuals whose data is involved, to control or even effectively monitor such transfers. These problems were not present in completely paper based systems, where the transfer of information about an individual was only through credential documents issued to the individual by one organization and shown by the individual to other organizations.

Cryptographic protocols that give individuals the ability to effectively control and monitor transfers in completely computer based systems, are presented. The essential idea is that an individual will be known to each organization by a different *pseudonym*, and that the individual will retain the exclusive ability to link the pseudonyms and transform digitally singed statements or *credentials* made about one pseudonym into credentials about the individual's other pseudonyms. Thus the individual regains control over inter-organizational transfers.

The Basic Credential System

The essential concept can be seen by analogy to carbon-lined window envelopes. First, you would make up your pseudonyms at random and write them on a plain slip of paper. When you

F. Pichler (Ed.): Advances in Cryptology - EUROCRYPT '85, LNCS 219, pp. 241-244, 1986.

want to get a credential from an organization, you put the slip of paper in a carbon-lined envelope with a window exposing only the part of the slip bearing the pseudonym you will use with that organization. Upon receiving the envelope from you, the organization makes a special signature in a repeating pattern across the outside of the envelope. The kind of signature pattern indicates the kind of credential the issuing organization decides to give based on the pseudonym they see through the window; the signature pattern serves as the credential. When you get the envelope back from the issuing organization, you verify the signature pattern. Before showing the credential to an organization, you place the slip in an envelope with a window position exposing only the pseudonym you use with that organization and some of the adjacent credential signature pattern. The receiving organization verifies the pseudonym and credential signature pattern recognizable through the window. This approach naturally allows a variety of credentials to be obtained and shown.

You need not show all of your credentials to every organization: you can restrict that which is revealed to only what is necessary. Because of the way the signature patterns repeat across the slip, a recognizable part of every signature pattern appears adjacent to each pseudonym. In providing an envelope to an organization, though, you can limit the view through the window so that only necessary signatures are visible. The credentials visible could simply be limited by blacking out parts of the window, but more flexible restriction is possible in actual systems. You could transform a credential representing your income, for instance, into a more restricted credential indicating only that your income falls within some range. An even more powerful kind of restriction allows an organization only to verify that you hold a combination of credentials meeting some requirement, without revealing anything to the organization about which sufficient combination you actually hold.

An organization can ensure that no individual is able to transact with it under more than one pseudonym. One way an individual could attempt to use more than one pseudonym with an organization is to use different pseudonyms on the same slip of paper. This is prevented by a standard division of the slip into zones, such that each zone is assigned to a particular organization; an envelope is accepted by an organization only if the window exposes the organization's zone, bearing a single indelibly written pseudonym. A second way of attempting to use more than one pseudonym per organization is to use more than one slip. This is prevented by the establishment of an "is-a-person" organization that limits each person to at most one is-a-person signature. Other organizations only accept envelopes with this signature recognizable through the window. This is-a-person organization might ensure that it issues no more than one signature per person by taking a thumbprint and checking before giving a signature that the print is not already on file. The collection of thumbprints poses little danger to individuals, since the is-a-person organization cannot link the prints with anything. The pseudonyms used by individuals are untraceable, in the sense that envelopes give no clue, apart from the signatures shown, about the other randomly chosen pseudonyms they contain. It is important to note that the actual cryptographic protocols provide unconditional untraceability using digital blind signatures on

numbers.

Credential Clearinghouses

When individuals have similar relationships with many organizations, there is often need for the centralized control provided by a *credential clearinghouse*, an organization that develops credential information about individuals' relationships with its member organizations and provides this information to these organizations. In current practice, clearinghouse functions are performed by such major organizations as credit bureaus, bank associations, insurance industry associations, national criminal information systems, and tax authorities.

For concreteness, consider how a credit clearinghouse might control the use of consumer credit using an extended form of the credential system. The clearinghouse gives you a number of *enabling* credentials that in effect say "This person is authorized for $100 worth of credit. If no resolution credential is returned to us within a year, we will assume that the individual has not repaid." You could provide one such credential to a shop, which then gives you credit worth up to $100. When you settle your account with the shop some time later, they give you the corresponding *resolution* credential, which you ultimately return to the clearinghouse. An important property of this approach is that the clearinghouse and shops cannot link the credentials; the clearinghouse with the cooperation of all the shops cannot learn which shop you went to, any more than the shop can learn your pseudonym with the clearinghouse, since the enabling and resolution credentials are unconditionally untraceable.

Security against abuse by individuals requires that the enabling credential be prevented from being shown to more than one shop. Otherwise someone could obtain too much credit from a single enabling credential. Similarly, it would not be possible to show a single resolution credential more than once to the clearinghouse, since otherwise someone could convince the clearinghouse that more debt had been repaid than was in fact repaid.

If individuals change pseudonyms periodically, they cannot be linked to obsolete information. Pseudonyms might be changed on a yearly basis. The initial information associated with new pseudonyms would be provided through the transfer of credentials from previous pseudonyms. The changeovers might be staggered to allow time for completion of pending business.

Conclusions

The techniques presented allow powerful, readily extensible, and flexible arrangements for exchange of information between organizations about individuals. They protect against abuses

by individuals, while providing unconditional security against linking of pseudonyms.

Reference

(1) Chaum, D., "Security without Identification: Transaction Systems to make Big Brother Obsolete" *Communications of the ACM*, 28, 10, (October 1985), 1030-1044.